Frédérick Douzet [*] : *« Si la dix-millième bombe peut être aussi efficace que la première, il n'en va pas nécessairement de même pour les cyber-attaques »*

(*) Maître de conférences à l'Institut français de géopolitique Membre de l'Institut universitaire de France

« Serait-il vraiment dans l'intérêt de la Chine d'anéantir les infrastructures vitales des Etats-Unis ? »

AeroDefenseNews : Cyber-sécurité, cyber-défense, cyberespace : difficile de s'y retrouver...

Frédérick Douzet : C'est normal car ces termes sont rarement clairement définis, il n'y a pas de véritable consensus sur une définition précise et les enjeux s'entremêlent. La cyber sécurité fait en général référence à la sécurité des systèmes d'information, des données, des programmes ou des ordinateurs contre les attaques, les intrusions non autorisées ou les dommages. Au sens plus large, elle vise à contrer les attaques criminelles qui se produisent par le biais des réseaux électroniques (escroqueries, piratage, vol ou destruction de données, etc.).

La cyber-défense concerne la protection contre les attaques menées par ou contre les réseaux d'information et de communication, et qui peuvent porter atteinte à la sécurité, à la souveraineté ou la puissance des nations. Or la distinction n'est pas toujours simple. Un même acte peut-être considéré comme cyber-criminel ou attaque stratégique en fonction de l'attribution et l'intention, autrement dit en fonction de qui est derrière l'attaque et pourquoi ? C'est justement ce qui est très difficile à déterminer et qui rend les stratégies des autres domaines militaires si difficiles à appliquer au cyberespace.

Le cyberespace lui-même est un terme flou. Ce n'est pas un espace au sens géographique du terme mais une représentation d'un espace, voire d'un territoire, qui n'est pas la même selon les acteurs. Cette représentation puise son fondement dans des mythes romantiques, à commencer par la vision futuriste de William Gibson, auteur du terme cyberespace, qui décrivait dans son roman Neuromancer dès 1984 cette *« hallucination collective »* dans laquelle les humains de toute la planète se rencontrent, conversent et échangent des informations. Ce sont aussi les mythes libertaires issus de la contre-culture des pionniers du Net, dont certains ont rédigé une déclaration d'indépendance du cyberespace, qui rejette la souveraineté des Etats sur ce monde de l'esprit. C'est encore le fameux *« Village global »* de Marshall McLuhan.

Cette représentation révèle aussi les rivalités de pouvoir qui opposent les acteurs (Etats, entreprises du secteur privé, pirates, criminels ...) dans une stratégie de conquête et d'appropriation de ce *« territoire »*, où l'on voit les Etats tenter de remettre un contrôle à leurs frontières pour réaffirmer leur souveraineté, faire respecter leur loi et assurer la protection de la nation. Ces frontières sont défiées aussi bien par les criminels, les associations de défense des libertés civiles, les multinationales, les dissidents, les hackers ou d'autres Etats. Il faut donc bien comprendre que ces représentations ne sont pas neutres, mais qu'elles ont une fonction dans les conflits géopolitiques

ADN : N'y a-t-il pas aujourd'hui une inflation de discours catastrophistes au sujet de la cyber-sécurité, de la cyber-défense ?

F. D. : On constate très clairement une inflation de discours catastrophistes, voire apocalyptiques à propos des dangers que recèle le cyberespace. C'est avant tout lié à la croissance exponentielle d'Internet, qui n'est plus l'affaire d'une élite pionnière mais devient accessible à tous ou presque, avec les risques que cela comporte. Les attaques contre les serveurs de l'Estonie en 2007, puis contre la Géorgie, le démantèlement du réseau Ghostnet qui a infecté les ordinateurs de 103 pays et dont la source provenait de serveurs chinois, puis la multiplication des attaques contre les entreprises et les administrations dans de nombreux pays ont suscité des inquiétudes croissantes et un sentiment de menace. On assiste à un véritable emballement politique et médiatique depuis 2009. Parce que l'ennemi est difficile à identifier, parce qu'il peut frapper à n'importe quel moment et n'importe où, parce que la technologie est abordable à un grand nombre d'individus, les cyber-attaques sont considérées comme l'arme du faible et incarnent le nouvel ennemi asymétrique. D'où le sentiment de menace.

ADN : La cyber-sécurité et la cyber-défense sont des thèmes d'actualité aux Etats-Unis. Quelle est leur approche ?

F. D. : L'administration Obama a nommé un *« Cyber Czar »*, un assistant spécial en charge de la coordination de la cyber-sécurité auprès de la Maison Blanche. En mai 2010, les Etats-Unis ont lancé le US Cyber command qui inclut toutes les composantes militaires, sous la responsabilité du directeur de la National Security Agency. Les initiatives législatives se multiplient pour renforcer la cyber-sécurité mais donnent lieu à de virulents débats politiques. D'une part, on assiste à un véritable clivage à tous les étages de la hiérarchie militaire et politique entre les alarmistes qui multiplient les analogies avec les armes de destruction massive et la guerre nucléaire et les sceptiques qui dédramatisent voire minimisent les risques spécifiques aux cyber-conflits. D'autre part, les mesures de défense et de sécurité relèvent nécessairement d'un équilibre entre surveillance des réseaux, sécurité et libertés civiques. Or, les différents acteurs qui participent au processus de décision ne partagent pas nécessairement les mêmes représentations ni les mêmes objectifs.

ADN : Les Etats-Unis considèrent désormais les cyber-attaques comme un acte de guerre. Quelles sont les conséquences concrètes d'une telle déclaration ?

F. D. : Cette déclaration est compréhensible dans le cadre d'une posture militaire dissuasive à l'égard des attaquants potentiels. Elle pose toutefois plusieurs questions : qu'est-ce qui constitue une cyber-attaque menaçant la sécurité du pays ? A partir de quel seuil la riposte est-elle légitime ? Qu'en est-il des cyber-attaques conduites par les Etats-Unis ? Autorisent-elles les autres nations à riposter par tous les moyens militaires contre le pays ? La révélation des auteurs du virus Stuxnet exacerbe ces enjeux ; les Etats-Unis ont à demi-mot reconnu avoir mené des attaques informatiques d'une envergure inédite contre le programme nucléaire du gouvernement iranien, et ce en collaboration avec Israël. Il va sans dire qu'il ne s'agit que de la partie émergée de l'iceberg.

ADN : Quels sont les risques potentiels et qui aurait intérêt à créer un tel chaos ?

F. D. : L'échelle d'évaluation des risques est justement ce qu'il faudrait définir pour développer une cyber-stratégie efficace. Or, on constate que beaucoup de ces discours sont plus souvent basés sur des fantasmes, sur des risques potentiels qui s'approchent parfois de la science fiction, et moins sur une analyse détaillée des campagnes de cyber-attaques. Le potentiel de destruction n'est pour l'instant pas démontré, de nombreux auteurs préfèrent utiliser le concept *« d'armes de perturbation massive »* et doutent qu'une cyber-attaque puisse conduire à des milliers de morts ou d'irrémédiables destructions matérielles.

La technologie qui est bien sûr largement accessible et nettement moins coûteuse qu'une armée, renforce l'idée de menace conduisant au chaos. Le cyber power accroît certes le pouvoir d'acteurs non-étatiques par rapport aux grandes puissances comme l'a théorisé Joseph Nye, mais il faut tout de même de longs mois de travail et des moyens non négligeables pour préparer une attaque de grande ampleur. Des entités comme des groupes terroristes ou un Etat peuvent ainsi développer la capacité de perturber ou neutraliser temporairement le fonctionnement de certains secteurs-clés d'un pays. Mais il est difficile d'imaginer qu'ils puissent mettre à terre une grande nation, voire simplement renouveler avec succès une attaque. Une fois la faille révélée, ce qui n'est pas toujours dans l'intérêt de l'attaquant, les réseaux peuvent être réparés et consolidés. Si la dix-millième bombe peut être aussi efficace que la première, il n'en va pas nécessairement de même pour les cyber-attaques.

ADN : La Chine est systématiquement montrée du doigt, est-ce justifié ?

F. D. : La Chine s'inscrit dans une logique de compétition internationale et d'affirmation de puissance, aussi bien dans le domaine économique que militaire ou technologique. Elle a clairement démontré sa capacité à maîtriser l'information dans le cyberespace, qui repose sur un mélange sophistiqué de technologie (en partie fournie par les grandes entreprises américaines), de méthodes ancestrales d'oppression (pression sur les intermédiaires pour la collaboration, surveillance, répression) et de propagande. De nombreuses attaques émanent de serveurs localisés en Chine et la nation est l'une des plus avancée dans la réflexion, avec une véritable intégration de la dimension cyber dans tous les aspects de la stratégie militaire. Elle considère la suprématie informationnelle comme l'un des multiples vecteurs de sa puissance. Mais les cyber-conflits n'existent pas en dehors des rivalités politiques du monde réel. Une cyber-attaque provoquant d'amples dégâts dégénérerait sûrement en conflit armé, de même que la dimension cyber est désormais une composante de tous les domaines militaires. Or, on peut poser la question : serait-il vraiment dans l'intérêt de la Chine d'anéantir les infrastructures vitales des Etats-Unis ? La vigilance est légitime dans le cadre des rivalités de pouvoir mais la focalisation sur la Chine peut faire oublier qu'elle est loin d'être la seule nation à conduire ces attaques.

ADN : Peut-on parler de dissuasion en termes de cyber-sécurité ?

F. D. : Bien sûr, à condition de ne pas faire d'amalgame avec la dissuasion nucléaire. Car le cyberespace possède ses propres caractéristiques et nécessite de développer des outils spécifiques pour les appréhender. Par exemple, la question de l'attribution des attaques est techniquement difficile et très coûteuse. Or, sans connaître à coup sûr l'auteur d'une attaque, sans preuve de ses intentions, quelle attitude adopter ? Riposter en prenant le risque de se tromper et de créer de nouveaux ennemis ? Ne pas riposter et se discréditer ? La question de la riposte se pose aussi si l'auteur est une force non étatique, impossible à désarmer ou qui n'a pas d'infrastructures à détruire en retour. Et encore une fois, la ligne de partage entre un acte de criminalité, d'espionnage ou de guerre n'est pas si facile à déterminer. Cela n'empêche pas les postures et les démonstrations de cyber power visant à décourager les attaques !

ADN : Comment jugez la situation en France et en Europe ?

F. D. : Les attaques de 2007 contre l'Estonie ont suscité une prise de conscience politique en France. La réflexion avance et se développe avec la reconnaissance de la sécurité des systèmes d'information comme enjeu de souveraineté de premier cercle par le Livre Blanc en 2008 et la création de l'ANSSI en 2009. En matière défensive, l'accent est mis sur le développement d'un retour aux fondamentaux de la sécurité comme en témoigne le récent guide *« d'hygiène informatique »* publié par l'ANSSI. En matière offensive, la France développe des moyens mais faut-il en faire état pour jouer la carte dissuasive ou rester discret ? L'enjeu au niveau européen est de parvenir à surmonter au moins en partie les rivalités politiques et économiques, ainsi que les enjeux respectifs de souveraineté et de sécurité source de méfiance, pour faire émerger une stratégie dans le cadre d'une coopération internationale. Il reste beaucoup à faire... ○●

Propos recueillis par Bruno Lancesseur

« Les mesures de défense et de sécurité relèvent nécessairement d'un équilibre entre surveillance des réseaux, sécurité et libertés civiques. Or, les différents acteurs qui participent au processus de décision ne partagent pas nécessairement les mêmes représentations ni les mêmes objectifs »

Bio Express

Frédérick Douzet est directrice adjointe de l'Institut Français de Géopolitique de l'Université Paris 8 et membre honoraire de l'IUF. Spécialiste des Etats-Unis, elle est l'auteure de *The Color of Power. Racial Coalitions and Political Power in Oakland* (University Press of Virginia, 2012) et avec Thad Kousser et Kenneth P. Miller, *The New Political Geography of California* (Berkeley Public Policy Press, 2008). Ses recherches portent sur les questions de géopolitique urbaine et les évolutions géopolitiques contemporaines de la Californie et des Etats-Unis. Elle s'intéresse aussi aux enjeux géopolitiques du cyberespace. Elle est membre du comité de rédaction de la revue de géopolitique Hérodote.